eIDAS as guideline for the development of a pan European eID framework in FutureID

Cuijpers, C.M.K.C.; Schroers, Jessica

Published in:
GI-Edition Lecture Notes in Informatics, 2015.

Publication date:
2014

Document Version
Early version, also known as pre-print

eIDAS as guideline for the development of a pan European eID framework in FutureID

Colette Cuijpers, Jessica Schroers

ICIS/ICRI
Radboud University/KU Leuven
Mailbox 47, P.O. Box 9010
6500 GL NIJMEGEN
cuijpers@uvt.nl
Jessica.Schroers@law.kuleuven.be

Abstract: *This paper addresses the Regulation on Electronic transactions in the internal market: electronic identification and trust services (eIDAS) and analyses this regulatory framework in relation to the pan European eID infrastructure being developed in the FutureID project. The aim of this paper is to identify if eIDAS sets forward any legal requirements that need to be implemented in the FutureID infrastructure. Even though the focus of this paper is on the development of the FutureID infrastructure, the description of eIDAS and the analysis of its main requirements for technical developers are in general relevant to the development of online identification and authentication schemes.*

1. Introduction

With the possibility to use the Internet for an abundance of services, between all kinds of different actors - consumers, businesses and government - there is a current need for reliable online identity authentication. Most online service providers use registrations and then username/password systems for their identity management. Such systems are bothersome for the users since they have to remember a lot of different passwords. Moreover, such systems are not very reliable for service providers.

Solutions for these problems can be found in a system of federated identity management, defined by Smedinghoff as an approach: "(…) where an enterprise engages in online transactions in reliance on identity credentials issued by any one of several third parties, and individuals can use the same identity credential to engage in transactions with multiple organizations." In simple terminology; a system of federated identity management makes it possible to answer the questions: "Who are you?" and "How can you prove it?" [S01]. The existing EU identity management landscape mainly consists of private initiatives on the one hand (e.g. Liberty Alliance Project/Kantara, OpenID), with the most familiar identification mechanism probably being log in with Facebook, Twitter and Google+ accounts. On the other hand, there are national public electronic identity schemes, which are often considered to be more reliable and trustworthy. Examples are the German nPA, the Austrian Citizen Card, the Belgian eID and the Dutch DigiD. These national systems are commonly used for national e-government services. There also exist public/private partnerships, mostly between banks and the government, whereby the government accepts the private identity means for their e-government services. This system is mostly used in the Nordic countries [ST02]. Besides existing eIDs there is a lot of research on how to develop more trustworthy eIDs. Mention can for example be made of biometric authenticated transactions in eBanking and eBusiness, which is promoted by both the European Payment Council (EPC) and the European Banking Union (EBU) [BRB03].

In view of internationalisation - one of the characteristics of the online environment - electronic authentication services preferably are not confined to national borders. As the examples above illustrate, in a lot of EU Member States national eID systems are (being) developed, based on the use of eID cards.[1] However, the legal international and European standardization[2] of citizen cards lags behind in the early deployments of eID systems in Europe, such as in Germany and Belgium, leading to a very diverse landscape of different eID cards for which an infrastructure is needed that supports all these cards across Europe. Different large scale EU funded projects aim to realize such infrastructure. In this respect mention can be made of projects such as: Stork, Stork 2.0 and FutureID.[3]

Besides all kinds of complexities and requirements regarding the technical development of the infrastructure, one other important design requirement concerns compatibility with existing legislation. In this paper we zoom in on a very recent legislative accomplishment, the Regulation on Electronic transactions in the internal market: electronic identification and trust services (referred to as eIDAS).[4] Before addressing eIDAS in section 3, we will first in section 2 provide a brief introduction into the mentioned projects, and explain why we focus on the FutureID project. In section 4 we will analyse whether eIDAS provides requirements that need to be implemented in the FutureID infrastructure. The aim of this paper is to provide the technical developers some guidelines regarding these requirements. Even though this paper focusses on the development of the FutureID infrastructure, the description of eIDAS and the analysis of its main requirements for technical developers are in general relevant to the development of online identification and authentication schemes.

2. EU eID projects

2.1 Brief Introduction

At the European level several projects are being carried out to develop a pan-European eID interoperability infrastructure.[5] While all these projects have a different focus or application domain, the common denominator is that these projects function as "Pillars for the development of interoperability of cross-border eID and trust. Identifying and using appropriate mechanisms to develop and engage "communities" – citizens and SMEs in particular - in promoting the use and uptake of eID and trust services".[6] The three main projects concerning the development of a cross-border infrastructure are Stork, Stork 2.0 and FutureID. Within these projects reference is made to a fourth project in which the concept of Attribute-Based Credentials is explored: ABC4Trust.[7] Attribute-based Credentials allow in a scenario of authentication to reveal only the minimal information required (e.g. this person is over 18), without giving away full identity information (e.g. this person is born on 19-04-1972). These credentials thus facilitate the implementation of a trustworthy and at the same time privacy-protecting digital identity management system.[8]

The project STORK[9] (Secure IdenTity acrOss boRders linked) was finished in 2012. The results of the project showed that it is possible to use national eIDs in cross border use cases by designing a system with two

[1] Part III of the Stork D2.2 report provides country reports concerning eID systems in the Member States.
[2] CEN TS 15480 and ISO/IEC 24727.
[3] Available 12 May 2014 at www.eid-stork.eu/; www.eid-**stork**2.eu/; www.futureid.eu/
[4] Official Journal of the European Union, L 257/73, 28.8.2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_257_R_0002&from=EN, available 10 September 2014.
[5] Without the aim of being exhaustive mention can be made of the following projects: STORK (https://www.eid-stork.eu/), STORK 2.0 (https://www.eid-stork2.eu/), SPOCS (http://www.eu-spocs.eu/index.php), PEPPOL (http://www.peppol.eu/), eCodex (http://www.e-codex.eu/home.html), epSOS(http://www.epsos.eu/).
[6] http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond
[7] https://abc4trust.eu/
[8] Available 12 May 2014 at https://abc4trust.eu/index.php/home/fact-sheet
[9] Available 12 May 2014 at www.eid-stork.eu

possibilities: either using the middleware so the user can communicate directly to the foreign system or using a Pan European Proxy Service (PEPS) which acts as a single gateway and intermediary for foreign eIDs towards domestic Service providers [WP04]. STORK 2.0 follows up on STORK and uses the system in additional pilots, including further also representation and mandates.[10]

While the eIDAS Regulation most likely has been written with the results of the STORK project in mind, we will focus our analysis on the FutureID project, in which we are involved as legal researchers. FutureID builds upon the findings in STORK and STORK 2.0 while also including the implementation of Attribute-Based credentials. Roßnagel et al. describe the project as: "The FutureID project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims [RCF05]". For users the interesting aspect of the project is that an eID is developed that can be used on ordinary desktop PCs, tablets and modern smart phones. From the perspective of service providers the advantage must come from an easy integration of existing services with the FutureID infrastructure. This will offer an effortless mechanism to benefit from strong security offered by eIDs without requiring service providers to make substantial investments. The idea is to offer the eID technology as a substitute for less secure alternatives currently in use such as username/password based systems. A third perspective described by Roßnagel et al. concerns existing and emerging trust service providers and card issuers "for which FutureID will provide an integrating framework, which eases using their authentication and signature related products across Europe and beyond."

2.2 Scope

As described above, FutureID concerns an infrastructure integrating and linking different technologies, different (trust) service providers and different users to facilitate cross border online identification and authentication, and make the use of electronic signatures easier in the form of a common eSignature framework that is capable to process digital signature related tasks, like signature creation and verification, with which different existing formats of advanced electronic signatures can be used [LR06]. In this paper we refer to the FutureID infrastructure, meaning the components being developed and offered within the scope of the FutureID project, while realising that a complete eID architecture consists of more, e.g. the actual provision of identification and trust services in the strict sense of the eIDAS Regulation. We consider the FutureID project merely to offer the technical components that together form the infrastructure necessary for online authentication and electronic signatures. As such, FutureID is not an entity or legal person capable to provide e.g. qualified signatures or certificates. Therefore, the establishment and provision of trust services such as qualified signatures and certificates falls outside the scope of the development of the FutureID infrastructure, being the focus of this paper. This means that the eIDAS requirements pertaining such services, signatures and certificates, will only be dealt with considering the infrastructure provision of the eSignature service.[11]

3. eIDAS

3.1 Background

The European Commission recognized the problem of not having a "comprehensive EU cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions that encompasses

[10] Available 12 May 2014 at https://www.eid-stork2.eu/

[11] E.g. we will not address the annexes I – IV of the Regulation concerning requirements for qualified certificates for electronic signatures, seals and website authentication, and requirements for qualified signature creation devices.

electronic identification and trust services".[12] In this respect, its Digital Agenda established an action on mutual recognition of electronic identification to provide a comprehensive and predictable legal framework in view of boosting user empowerment, convenience and trust in the digital world.[13] Providing such a legal framework is a necessary precondition to achieve modernization in public administration, mentioned in the European Commission's 'Annual Growth Survey 2013' as "one of the five priorities for the Member States in the next 12-18 months (….). To underpin the digital transition in public services and to ensure they are available to all Europeans regardless of their place of residence, the Commission envisages deploying and rolling out digital services in key areas of public interest" [EC07].

The revision of the eSignature Directive (1999/93/EC) started on the 4th of June 2012 with a proposal of the European Commission for a Regulation on **e**lectronic **ID**entification and **A**uthentication **S**ervices (eIDAS). In February 2014 the representatives of the European Parliament (MEP), the Commission and the Council reached a political agreement regarding eIDAS.[14] The proposed Regulation was adopted by the MEP with 534 votes in favor, 73 against and 7 abstentions, on the 3rd of April 2014.[15] The Regulation has been adopted by the Council on the 23rd of July 2014. It is officially published in the OJ on the 28th of August 2014.[16] The eSignature Directive will be repealed with effect from July 1, 2016, which is also the date from when the Regulation shall apply.[17] In order to make the transition smooth, some transitional measures are established. For example, qualified certificates issued under the eSignature Directive will be considered as qualified certificates until they expire.[18] A certification service provider issuing qualified certificates has to submit a conformity assessment report and shall then also be considered as qualified trust service provider under the Regulation.[19]

3.2 Main problems addressed by eIDAS

Derived from the key actions in the Digital Agenda mentioned above, the Regulation wants to address two problems. The first is that citizens can't use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes are not recognized in other Member States. This makes it difficult for all cross-border online services for which a higher level of trusted identification and authentication is necessary in order to be used, like for example cross-border healthcare or online public procurement.

The second problem that the Regulation will address is the diverging legal validity of trust services. Trust services are electronic services *"which consist of:*

(a) The creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to these services, or
(b) The creation, verification and validation of certificates for website authentication; or

---

[12] Wording taken from the explanatory memorandum of eIDAS, available 12 May 2014 at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0238.
[13] See action 8 (revision of the eSignature Directive) in combination with action 83 (mutual recognition of electronic identification), available 12 May 2014 at http://ec.europa.eu/digital-agenda/en/pillar-i-digital-single-market/action-8-revision-esignature-directive
[14] Available 12 May 2014 at http://europa.eu/rapid/press-release_MEMO-14-151_en.htm
[15] Available 12 May 2014 at http://www.europarl.europa.eu/pdfs/news/expert/infopress/20140403IPR41931/20140403IPR41931_en.pdf
[16] Official Journal of the European Union, L 257/73, 28.8.2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_257_R_0002&from=EN
[17] Art. 52 eIDAS.
[18] Art. 51 (2) eIDAS.
[19] Art. 51 (3) (4) eIDAS.

(c) *The preservation of electronic signatures, seals or certificates related to these services."*[20]

One of the points of criticism on the eSignature Directive was that it only focuses on electronic signatures and leaves out other important trust services. This criticism has been taken up in the Regulation and it provides now also a framework for electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

3.3 Approach of the Regulation regarding the problem of electronic identity

The Regulation does not try to introduce a common European electronic identification system. This would be problematic since identification of citizens is a core national sovereignty. Instead, it provides for the possibility of cross-border use and mutual recognition of existing systems of the Member States by giving them the option to notify their electronic identification scheme to the Commission. The notification is only possible if the scheme fulfils certain criteria and is not obligatory for the Member States.[21] Member States are obliged to accept notified identification means of others if their own online public services can be accessed by electronic identification means.[22] They can start joining the system from July 1, 2015.[23] In section 3.5 we will discuss the liability regime regarding notified identification means.

The obstacle in mutual recognition is that not all Member States identification means have the same security levels. Member States, which have more secure means for accessing their online service, don't want to accept less secure means of other Member States. To enhance the trust of the Member States in each other's notified schemes the Regulation provides for 3 'Identity assurance levels'. These will be addressed in section 4.3.

3.4 Approach of the Regulation regarding Trust Services

The Regulation now provides for a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and qualified certificates services for website authentication. This is a closed list of trust services, but Member States remain free to recognize at a national level other types of trust services as qualified and maintain or introduce national provisions to non-harmonized trust services.[24]

The non-discrimination rule of the Directive applies in the Regulation also to the mentioned trust services (except the qualified certificates for website authentication), which means that those trust services can be used as evidence in legal proceedings.[25] But it is still up to national law to define the legal effect of trust services, except where the Regulation states the effect.[26] The Regulation permits for trust service providers complying with the Regulation to circulate their products freely in the internal market, but also includes liability of trust service providers, which will be discussed in the next section. Member States will establish trusted lists with information on the qualified trust service providers.[27] If a trust service provider is on such list it may use the EU trust mark.[28] Qualified trust service providers will be supervised by a designated national supervisory body, which will also take action if non-qualified trust service providers allegedly do not meet the requirements of

[20] Art. 3 (16) eIDAS.
[21] Art.7 and 9 and recital (13) eIDAS.
[22] Art. 6 eIDAS.
[23] Committees Committee on Industry, Research and Energy, Plenary sessions [03-04-2014 - 13:36] available 12 May 2014 at http://www.europarl.europa.eu/pdfs/news/expert/infopress/20140403IPR41931/20140403IPR41931_en.pdf
[24] Recitals (25) and (24) eIDAS.
[25] Recital (22), art. 25, art. 35, art. 41, art. 43, art. 46 eIDAS.
[26] Recital (22)
[27] Art. 22 eIDAS.
[28] Art. 23 eIDAS.

the Regulation.[29] Section 3.6 will elaborate on the extended supervision in the Regulation compared to the Directive.

3.5 Approach of the Regulation regarding Liability

One of the crucial issues of eIDAS concerns the allocation of liability.[30] Liability for trust services is rather straightforward. Art. 13 states that trust service providers are liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. The intention or negligence of a qualified trust service provider shall be presumed unless a qualified trust service provider proves otherwise. The burden of proof regarding a non-qualified trust service provider lies with the claimant.

More interesting and questionable is the liability provision of Art. 11 eIDAS. Besides strict liabilities for the party issuing electronic identification means and the party operating the authentication procedure, strict liabilities also pertain to notifying Member States.[31] These Member States are liable for damage caused intentionally or negligently to any natural or legal person when the availability of online authentication is not ensured, or when it is not ensured that the person identification data uniquely represent the person in question. This only relates to cross border transactions in which it must be ensured that electronic identification means is attributed "in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8".[32] The liability of the notifying state has raised several critiques [DV08] [V09]. It is questioned whether the Member States will take responsibility for other parties than the State itself to provide online identification and authentication services. This does not conform to the market approach that is expressed in Recital 13 of eIDAS: "Member States should remain free to use or introduce means, for electronic identification purposes, for accessing online services. They should also be able to decide whether to involve the private sector in the provision of these means". It could even lead to Member States abstaining to notify electronic identification schemes, blocking the possibility of mutual recognition of such systems. Dumortier and Vandezande from a different perspective point to barriers for private parties to enter the online identification market, as service providers may have to make substantial investments in order to comply with the liability requirements [DV08].

3.6 Approach of the Regulation regarding supervision

The eSignature Directive referred to supervision only in one article stating that each Member State shall ensure the establishment of a supervision system for qualified certification service providers[33], which resulted in a variety of supervision schemes in different Member States.[34] In response to this the Regulation contains much more extensive supervision provisions, however, supervision in eIDAS is only specified for trust services. The supervision remains at the national level, so there is no European supervisory body, but Member States designate a supervisory body in their territory with the necessary powers and adequate resources.[35] These supervisory bodies are considered to cooperate with each other and only in case of security breach with a cross border dimension ENISA will be informed.[36] In general is it the role of the supervisory body to ensure that the requirements of the Regulation are followed by supervising qualified trust service providers and taking action in case non-qualified trust service providers do not meet the requirements.[37] Penalties for infringements of the

[29] Art. 17 eIDAS.
[30] Recitals (18) and (37). Art. 11 and 13 eIDAS.
[31] Art. 11 eIDAS.
[32] Assurance levels are discussed in section 4.3.
[33] Art. 3 (3) eSignature Directive.
[34] Feasibility study, p. 57.
[35] Art. 17 eIDAS
[36] Art. 18, art. 19 eIDAS.
[37] Art. 17 lid 3 eIDAS.

Regulation are up to the Member States assessment.[38] To ensure the conformity of the qualified trust service providers they shall be audited at least every 2 years and additionally the supervisory body may always request another audit or audit themselves.[39] The Commission may specify which standards should be followed for the audit.[40] For electronic identity the Regulation provides no independent supervision system that would guarantee a uniform level of protection [see [SR10, p. 144][BHM11]. Even after the modifications of the Regulation this is still the case]

4. Requirements of eIDAS for the development of FutureID

4.1 Introduction

In this section we address the requirements that can be derived from eIDAS that need to be taken into consideration in the technical development of the FutureID infrastructure. As explained and defined in section 2.2, we will focus the analysis of the requirements to the FutureID infrastructure.

4.2 Privacy and Data Protection

Privacy awareness and the need for adherence to strict privacy rules gained momentum in the development of eIDAS as can be witnessed by the fact that the current version of eIDAS, as accepted by Parliament, contains stronger data protection requirements than the original proposal of the Commission.[41] Recital 11 concerns a general obligation to apply the Regulation in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC.[42] Without addressing all the requirements that stem from this Directive, the recital does stress the need for data minimisation: "authentication for a service online should concern processing of only those identification data which are adequate, relevant and not excessive to grant access to that service online". In relation to trust service providers and supervisory bodies eIDAS explicitly states that the requirements of confidentiality and security must be respected.[43]

Article 12 of eIDAS concerns notified national electronic identification schemes. After establishing the requirement of interoperability of these schemes, the article requires further that the interoperability framework shall meet the following criteria in relation to data protection:

"(c) it shall facilitate the implementation of the principle of privacy by design; (d) it shall ensure that personal data is processed in accordance with Directive 95/46/EC".

Even though eIDAS stresses the need to incorporate privacy requirements into the architectural design of electronic identification schemes, the details of what these requirements entail are not part of eIDAS.

It was even feared that some provisions of the eIDAS Regulation would prohibit the notification of special privacy advancing solutions, like the solution of the German nPA with mutual authentication requirement and user-centric transfer of personal data using a certificate that is subject to costs [BHM11] [Q-K12]. Art. 6 about

[38] Art. 16 eIDAS.
[39] Art. 20 eIDAS.
[40] Art. 20 (4) eIDAS.
[41] Original proposal available 12 May 2014 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:en:PDF.
[42] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31.
[43] Recital 11 eIDAS.

the notification requirements has been adjusted and, in the last version, no longer requires that the Member State ensures the availability of the authentication possibility at any time, free of charge and for any relying party, but restricts it for services online provided by a public sector body and specifies further that Member States shall not impose any specific disproportionate technical requirements on relying parties where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes (art. 7 (f)).

Data minimisation, confidentiality and security are only a few of the requirements stemming from an extensive EU legal framework regarding data protection.[44] All requirements of this legal framework must be taken into account in developing the FutureID infrastructure. However, it goes beyond the scope of this paper to discuss all the relevant data protection requirements. These requirements stem from a different legal framework, while the focus of this paper is to address requirements stemming from eIDAS. Moreover, the EU legal framework regarding data protection is currently under review, replacing Directive 95/46/EC with a Regulation. More clarity on the exact provisions of the Data Protection Regulation is expected later this year, or even next year, as the Council has postponed its hearing until after the elections of May 2014.[45] Presumably, the text the Council ultimately approves will contain amendments to the text adopted by the Parliament.[46] In view of the explicit reference in eIDAS to the principles of privacy by design and privacy by default, we do want to stress the importance to try and build into the FutureID infrastructure privacy requirements that can be derived from the current *and* prospective EU legal framework regarding data protection.[47] At this point in time, however, it is difficult to predict what the exact implications of these new principles will be. To give an example we point to the current developments in the Netherlands. Dutch government is still in the process of developing a coordinated, national system of electronic identities, including a publicly eID card with a high level of reliability. An interesting question the principles of Privacy by Design and Default raise, concerns the room for Dutch government not to make use of certain technologies, such as attribute based credentials, if experts agree such tools to be the most privacy-friendly solution. [LDP15]

Besides the requirements pertaining to data protection, article 12 furthermore demands the interoperability framework to be technology neutral and non-discriminatory between any specific national technical solutions for electronic identification within the Member States. These requirements, just as data protection and privacy compliance, are explicitly stated to be the main goals of FutureID, and thus are an integral part of the technical development strategy of FutureID. A final requirement of Article 12 concerns the obligation to follow, when possible, European and international standards. This requirement is the subject of the next section.

4.3 Assurance levels and standards

Even though art. 12 does not in a strict sense oblige developers of FutureID to adhere to assurance levels and standards as some room is left in the phrasing: “when possible”, we do address them as it will offer great advantages to implement these assurance levels into the FutureID infrastructure since these levels will provide one common European system.

Depending on the negative impact of a wrong authentication the risk level of a service can vary [J16]. For this reason different national governments and several EU projects defined frameworks that specify different

[44] Currently consisting of Directive 95/46/EC, but also the ePrivacy Directive (2002/58/EC as amended by 2009/136/EC) and the Data Retention Directive (2006/24/EC).
[45] See http://europa.eu/rapid/press-release_MEMO-14-186_nl.htm
[46] Text adopted by the Parliament available 12 May 2014 at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf and http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf.
[47] More on the revision of the data protection legal framework and privacy by design [K13] [CKP14].

Authentication Assurance Levels (AAL) for user authentication, to balance different levels of risk with corresponding appropriate authentication assurance [J16]. Also in eIDAS the EU legislator has defined 3 different assurance levels: "low", "substantial" and "high".[48] "Low" provides a limited degree of confidence and its aim is to decrease the risk of misuse and alteration of the identity, while the purpose of "substantial" is to substantially decrease the risk.[49] "High" will provide the highest level of confidence and its purpose is to prevent misuse or alteration of the identity.[50] Only means with an equal or higher assurance level than the level required for the online service can be used to access the service, so it will not be possible to access a high level online service with low level identification means.[51]

These criteria are quite vague and to specify them the Commission provides that, ultimately 12 months after entry into force of the Regulation, the Commission shall by implementation acts set out minimum technical specifications, standards and procedures.[52] These shall be established by reference to the reliability and quality of the identity registration (identity proofing, issuance procedure, issuing entity), the authentication method (which mechanism is used) and the specifications of the issued electronic identification means.[53] Despite the fact that no implementing acts are available yet, the direction in which these will go are clear. Recital 16 of the Regulation refers to the Large Scale Pilot STORK[54] and ISO 29115[55] and inter alia, to their levels 2, 3 and 4, "which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurances levels low, substantial and high within the meaning of this Regulation, while ensuring consistent application of this Regulation in particular with regard to assurance level high related to proofing of identity for issuing qualified certificates."[56] eIDAS also states that requirements should be technology neutral and that "it should be possible to achieve the necessary security requirements through different technologies."[57]

The implication for pan European eID frameworks lies less in how the exact definition of the assurance levels is and more in the fact that there will be binding levels for notified eID means and that those will be specified. While in case of only national eID systems the service provider normally can assess the reliability and trustworthiness of their well-known own national eID, this is not the case for eIDs from other Member States. Therefore, pan European eID frameworks need to provide a solution for this problem and assurance levels are there for this reason. However, currently it is problematic that there are different assurance level systems and different ways to map them. The implementation acts of the Regulation will now set out three levels with hopefully clear specifications. Additionally, the Member States who notify their schemes must indicate the assurance level and they have to ensure that the means have been attributed to a person in accordance with the technical specifications, standards and procedures set out by the implementing acts.[58] This provides a high grade of reliability for pan European eID frameworks and service providers. However this will still be only for government notified eID schemes, therefore a reliable system for private eID solutions is not defined by the eIDAS Regulation [SR10, p. 45]. Nevertheless also private eID providers, whose schemes are not notified can

[48] Art. 8 eIDAS.
[49] Art. 8 (2) (a) and (b) eIDAS.
[50] Art. 8 (2) (c) eIDAS.
[51] Art. 6 (1) (b) eIDAS.
[52] Art. 8 (3) eIDAS.
[53] Recital 16 and Art. 8 (3) eIDAS. See also [J16, p. 75].
[54] Described in STORK D2.3, Quality authenticator scheme, available 12 May 2014 at https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312. The STORK Quality Authentication Assurance (QAA) model defines 4 assurance levels (named 1: no or minimal assurance, 2: low assurance, 3: substantial assurance and 4: high assurance).
[55] ISO/IEC 29115:2013 Information technology-Security techniques-Entity authentication assurance framework. ISO29115 provides also 4 levels of assurance (called LoA 1 low; LoA 2: medium; LoA 3: high and LoA 4: very high).
[56] Recital (16).
[57] Recital (16).
[58] Art. 9 (1) (a), art. 7 (e).

use the assurance level system in cross-border situations, therefore the assurance levels can provide a framework also for not notified eID solutions.

4.4 Usability

To conclude this section on requirements, we address usability and user friendliness. Recital 47 of eIDAS states that: "Confidence in and *convenience of* online services are essential for users to fully benefit and consciously rely on electronic services" (emphasis added). Even though this sentence is the introduction to create an EU trust mark, it also hints to usability and user friendliness as more general requirements in the development of online identification and authentication schemes. Article 15 of eIDAS concerns the usability of a specific group of users, as it requires, where feasible, the accessibility for persons with disabilities. This requirement does not only pertain to trust services, but also to end user products used to provide these services. This is an important requirement for the eSignature service of FutureID which should be taken into account.

5. Conclusion

eIDAS does not contain a lot of requirements directly relevant to the development of the FutureID infrastructure. This mainly relates to the scope of the FutureID project and the fact that a substantial part of eIDAS is focused on the actual provision of Trust Services. The main goals of the FutureID infrastructure align with important focus points of eIDAS, such as interoperability and compliance with data protection. Even though the relevance of eIDAS for the development of FutureID as such is limited, the implications of eIDAS for the overall pan European online authentication environment are substantial. At this point it is hard to predict whether eIDAS will indeed lead to a vivid cross border electronic identification and authentication landscape. The eSignatures Directive was stipulated as 'used by few and ignored by many' [DV08, p. 19], if this will change with the Regulation relates e.g. to the existence of actual use cases and how the liability regime of eIDAS will affect the mutual recognition of online identification and authentication schemes. Liability for notifying Member States may cause barriers for private parties to enter the market and could even lead Member States to abstain from notifying any scheme.

References

[S01] Smedinghoff, T.J., Solving the legal challenges of trustworthy online identity, Computer Law & Security Review 28 (2012) p. 532.

[ST02] STORK D2.2 Report on legal interoperability, p. 152, available 12 May 2014 at https://www.eid-stork.eu/dmdocuments/public/D2.2_final._1.pdf

[BRB03] Buchmann, N.; Rathgeb, C.; Baier, H.; Busch, C.; Towards electronic identification and trusted services for biometric authenticated transactions in the Single Euro Payments Area, in Proceedings of the 2nd Annual Privacy Forum (APF'14), 2014, p. 172.

[WP04] Written report of the Article 29 Data Protection Working Party Biometrics & eGovernment Subgroup on STORK, available 12 May 2014 at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_15_letter_artwp_atos_origin_annex_en.pdf

[RCF05] Roßnagel, H.; Camenisch, J.; Fritsch, L.; Gross, T; Houdeau, D.; Hühnlein, D.; Lehmann, A.; Shamah, J.; FutureID – Shaping the Future of Electronic Identity, p. 1, available 12 May 2014 at http://ec.europa.eu/digital-agenda/events/cf/ict2013/document.cfm?doc_id=25733

[LR06] Lipp, P.; Rath, C.; et. al.: "FutureID D33.1 Requirements Report". Available at 10 September 2014 at http://www.futureid.eu/data/deliverables/year1/Public/FutureID_D33.01_WP33_v1.0_Requirements%20Report.pdf.

[EC07] European Commission Annual Growth Survey, Brussels, 28.11.2012, COM(2012) 750 final.

[DV08] Dumortier, J.; Vandezande, N.; Critical Observations on the Proposed Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (September 26, 2012). ICRI Research Paper 9. Available at 12 May 2014 at SSRN: http://ssrn.com/abstract=2152583.

[V09] Voulon, M.B.; Een Europese verordening voor identity management (IdM), Computerrecht 2013/118, p. 196-204.

[SR10] Spindler, G.; Rockenbauch, M.: Aufsatz, Die elektronische Identifizierung, MMR 2013, p. 138-149.

[BHM11] Byszio, F.; Houdeau, D.; Meister, G.; Wolfenstetter, K-D.: Aufsatz, Elektronische Identifikation in Europa: die neue EU-Verordnung, DuD 2013, p. 171.

[Q-K12] Quiring-Kock, G.; Aufsatz, Entwurf EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, DuD 2013, 20-24, p. 21.

[K13] Kuner, C.; The European Commission's Proposed Data Protection Regulation: A Copernican revolution in European data protection law (2012) 11 Privacy & Security Law Report 6, 1–15.

[CKP14] Cuijpers, C.; Kosta, E.; & Purtova, N.; Data Protection Reform and the Internet: The Draft Data Protection Regulation. In Savin, A.; Trzaskowski, J.; (eds) Research Handbook on EU Internet Law. Cheltenham: Edward Elgar, p. 543-568.

[LDP15] Ministry of the Interior and Kingdom Relations, Dutch eID system. Strategic Outlook and proposal for follow-up. Available at 15 September at http://www.eid-stelsel.nl/fileadmin/eid/documenten/20130812_Strategic_Outlook_and_proposal_for_follow-up_eID_Stelsel.pdf

[J16] Jøsang, A.; Identity management and trusted interaction in Internet and mobile computing, IET Information Security, Vol. 8, Iss. 2, 2014, pp. 67-79.